Mitel One

VERSION 2.0

SECURITY GUIDELINES

APRIL 2023

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

Mitel One
Security Guidelines
Version 2.0
April 2023

Overview

This document provides an overview of the security mechanisms used by the Mitel One application to counter threats and to ensure user data privacy. It describes the security features of the Mitel One system design that ensure secure deployment and operation of the Mitel One application and relevant add-ons.

The Mitel One application is a desktop web browser application that allows a user to communicate (Unified Communications (UC) and meetings) with other web application users from the same company account.

The Mitel One web application also allows users to make and receive external voice calls. To establish external communication channels, the Mitel One web application utilizes the Mitel CloudLink (CL) Platform, which also provides additional security features.

The security features of the Mitel CloudLink Platform include user authentication and authorization, secure Cloud API access, protection of cloud data used by the application, encrypted signaling, secure event notifications, and secure reporting of software logs.
Mitel has clearly defined IT security policies in place that define goals, assets, trust levels, processes, and incident handling procedures. The security procedures implemented in the Mitel One application solution are covered by and configured according to these policies. The security principles of Mitel One are:

- **Secure by Design**: The Mitel One application is designed and developed using the Mitel Secure Development Life Cycle process. For more information, see the Mitel Secure Development Life Cycle whitepaper available on the Mitel Document Center at https://www.mitel.com/en-ca/document- center/security/technical-papers.
- **Secure by Default**: Data in transit is encrypted by default using Transport Layer Security (TLS 1.2 or later) and Web Real-Time Communication (WebRTC) protected by 256-bit or higher Advanced Encryption Standard (AES) encryption. Data at rest is protected by 256-bit or higher Advanced Encryption Standard (AES) encryption in Amazon Web Services (AWS) cloud.
- **Built on a Secure Platform**: The Mitel One application is empowered by services provided by Mitel's CloudLink platform. See https://www.mitel.com/en-ca/document-center/technology/cloudlink-security for more details.
- **Identity Access Management (IAM)**: Mitel's CloudLink IAM solution supports Open ID Connect and OAuth 2.0. For information about identity access control, refer to the Identity Access section later in this document.

About the Mitel One Documentation Set

For complete information about the Mitel One application, refer to https://www.mitel.com/document-center/applications/collaboration .

Product documentation for all CloudLink products is available at https://www.mitel.com/document-center/technology/cloudlink .

Other Mitel® product documentation is available in the Mitel Document Center.

Product Architecture

The Mitel One application is a CloudLink-based remote / mobile solution designed for users who want to improve work efficiency, enhance workplace communication, and provide a highly connected customer experience. The end-user experience is realized through a secure desktop, web, or mobile client delivering Unified Communication and contact center features.

Mitel One uses services provided by the Mitel CloudLink platform including voice, chat, cloud user directory, user presence, user call history, user authorization and authentication, workflow, reporting, and entitlements. The Mitel CloudLink platform utilizes AWS to offer customers a Platform as a Service (PaaS). The Mitel One application uses the Internet to transport data such as voice, files, audio, chat, and reports.

The following is a schematic diagram of the Mitel One application solution architecture.

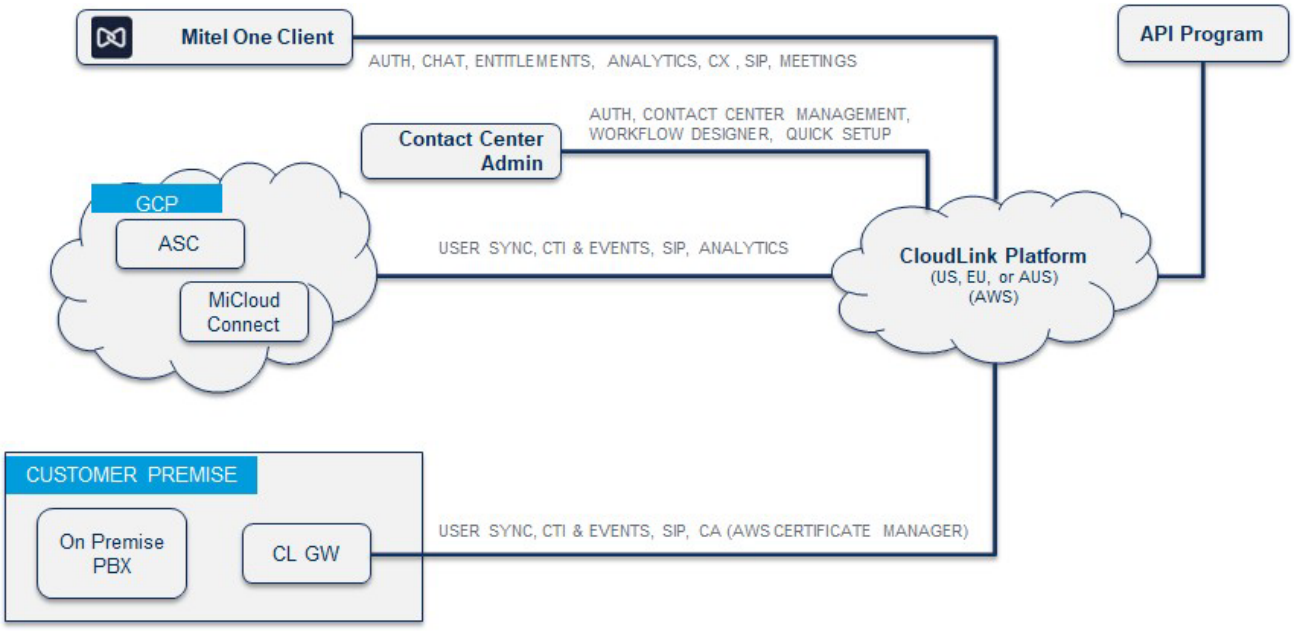

Figure 1: Mitel One Application Solution Architecture

Client Security

The security framework for the Mitel One solution includes:

- Data in transit is encrypted by default using Transport Layer Security (TLS 1.2 or later) and Hypertext Transfer Protocol Secure (HTTPS) to provide secure endpoint communication.
- Web Real-Time Communication (WebRTC) is protected by 256-bit or higher Advanced Encryption Standard (AES) encryption.
- Secure Real Time Protocol (SRTP) is used to secure media streams (AES 256 encryption).
- Data at rest is protected by 256-bit AES encryption.
- CloudLink Identity Access Management (IAM) to provide a single trusted location for users. CloudLink IAM uses CloudLink's native IAM solution, which supports Open ID Connect 1.0 and OAuth 2.0.

The Mitel CloudLink platform implements user password rules derived from NIST 800-63. Users are forced to change the system-generated password provided in the welcome email that they receive for accessing the application on initial login. The password must contain:

- between 8 and 128 characters
- at least one special character (@ ! # $ % & _ - = +)
- at least one digit
- at least one uppercase letter and one lowercase letter.

Shared Responsibility Model

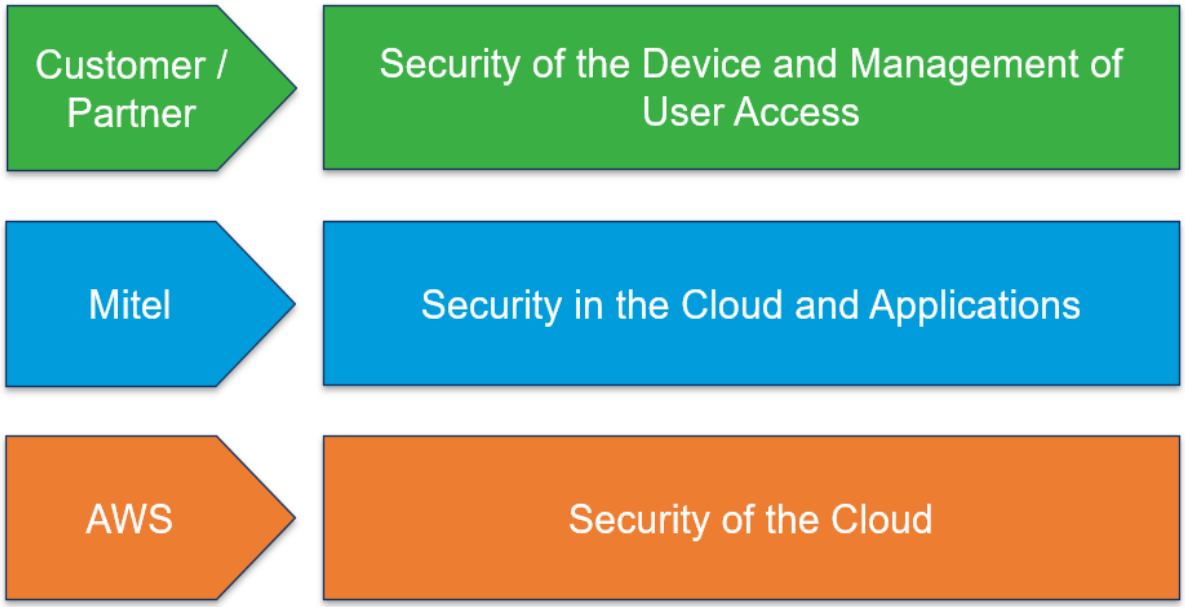

Figure 2: Shared Responsibility Model

The shared responsibility model is discussed in the CloudLink Security FAQ .

The Shared Responsibility Model is based on the AWS Shared Responsibility Model (“Shared Responsibility Model - Amazon Web Services (AWS)” Amazon Web Services (AWS) - Cloud Computing Services, Amazon.com, Inc., 14 September 2021.) since it is the Platform as a Service provider for CloudLink. As defined by the model, AWS is responsible for the “Security of the Cloud”. Mitel is responsible for “Security in the Cloud” for the aggregate services and applications that Mitel provides. The customer/partner also has a key role in that they are responsible for the security of their own devices and the access they provide their users on those devices. Mitel recommends that the customer/partner fully understand and apply the best security practices as stated by the device manufacturer and Operating System supplier.

Identity Access

As shown in the following diagram, identity Access Control utilizes a shared responsibility model between the CloudLink Platform, Mitel applications and the customer. The CloudLink platform is responsible for ensuring secure access to the AWS foundation services used by the CloudLink platform, restricting such access to Mitel employees, and limiting access to a specific job function. The best practices employed include the use of AWS Organizations, Role Based Access Control (RBAC) for limiting access to job functions of personnel, Multi- Factor Authentication for accessing AWS infrastructure, and dedicated security accounts in AWS (to ensure security events are monitored by the correct personnel).

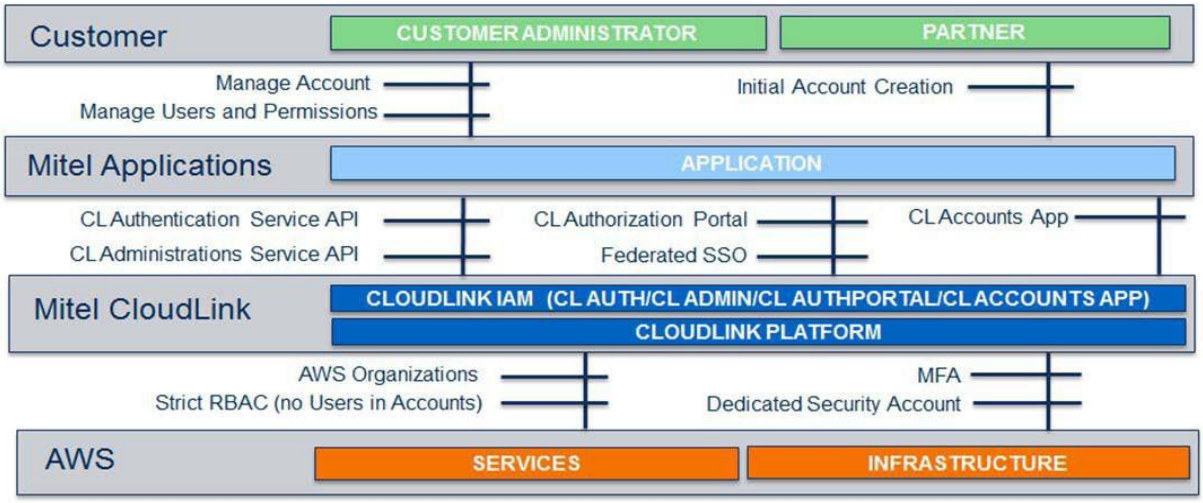

Figure 3: Identity Access

Mitel applications are designed to ensure that identity and access related to application accounts and users are accurately reflected within the CloudLink platform. Mitel applications perform these functions through secure APIs provided by the CloudLink Identity Access Management (IAM) solution. The IAM solution is designed to ensure access to services and data is isolated to the appropriate account and limited to the responsibilities of the users defined by the customer.

The CloudLink IAM solution is an open solution based on Open ID Connect 1.0 with support for federated single sign-on (SSO) using SAML 2.0. The CloudLink IAM solution offers a common login portal (CloudLink Authorization Portal), which Mitel applications use for SSO requirements.

The partner/customer is responsible for managing the company account, users, and permissions to the overall solution.

NOTE: A certified Mitel partner is required to initially create the customer account in CloudLink from the CloudLink Accounts application. All cloud data used in the web application is stored on the Mitel CloudLink platform and is identified with company account ID, user ID and other globally unique identifiers associated with a fully authenticated and verified account.

Access Control Matrix

Feature	Partner Admin	Customer Admin	User	Guest
Mitel One User Features				
WebRTC Phone with multi-line support	Full Control[2]	Full Control[2]	Full Control[2]	N/A
Voice Features	Full Control[2]	Full Control[2]	Full Control[2]	N/A
Calendar	R	R	R	N/A
Personal direct messaging	Full Control[3]	Full Control [3]	Full Control [3]	N/A
	Full Control[3]	Full Control [3]	Full Control [3]	N/A
Streams				
Corporate Directory Integration and Global Search Functionality	R, X	R, X	R, X	N/A
Microsoft AD SSO	Full Control	Full Control	R, X	N/A
Control the call features on the MiVoice Office 400 desk phone	R, M, X	R, M, X	R, M, X	N/A
Do Not Disturb (DND)	R, M, X	R, M, X	R. M. X	N/A
Live status (presence) of users	R, M[4]	R, M[4]	R, M[4]	N/A
Dynamic Call History	R	R	R	N/A
Contact synchronization and management	R, X	R, X	R, X	N/A
Favorites	Full Control	Full Control	Full Control	N/A
Mitel One Meetings Integration User Features				
Video Conference	Full Control	Full Control	Full Control	X
Screenshare	X	X	X	X
Meetings Chat	Full Control[3]	Full Control[3]	Full Control[3]	C, R
Record meetings	R, C, D, X	R, C, D, X	R, C, D, X	N/A
Create an Ad Hoc Meeting	C	C	C	N/A
Schedule a Meeting	C	C	C	N/A
Search a Meeting	X	X	X	N/A

Create invite-only meeting	C	C	C	N/A
Join a Meeting	X	X	X	X
Leave a Meeting	X	X	X	X
Meeting Controls	M, X	M, X	M, X	M, X
Integration with Office 365 Calendar and Meetings	C, M	C, M	C, M	N/A
Meetings Outlook Add-in	C, M	C, M	C, M	N/A
Delete a Meeting	D	D	D	N/A

Notes:

- The access of each user role (Partner Admin, Customer Admin, User) is isolated to their own tenant/account.
- User generated content is restricted to the creator of the content and the authorized recipients of the content.
- Guest users are not registered with the system.
- [1] The Partner Administrator can perform an assume role operation to access the administration feature on behalf of their customer.
- [2] Access may be limited due to feature restrictions of the PBX/Call Control Engine.
- [3] Modify and delete permissions for Chat are set on a per account basis.
- [4] Can modify only the user's own status.
- [5] For a registered user.
- The table below assumes the user has been licensed for the feature.
- Access terminology:
    - R = Read
    - C= Create
    - M = Modify
    - D = Delete
    - X = Execute
    - Full Control = R, C, M, D, X
    - N/A = Not Allowed

Messaging

Mitel One offers multiple messaging systems with attachment capability to meet individual customer needs. This includes:

Personal direct messaging: one-to-one messaging (chats) and group chat messaging capability.

- Streams messaging: Streams messaging is a chat-based collaboration space
- Meetings messaging: Meetings is a video collaboration tool with video, audio, and chat capabilities.

Chats

- All messages are accessible only by the participants of the direct, stream, and meeting space.
- Unless the Edit/Delete feature is disabled by the corporate administrator, chat messages can be edited and/or deleted by the sender. The Edit/Delete feature is enabled by default. If the recipient had replied to a message that is being deleted, the original content of the message is still retained in the reply.
- Unless deleted by the sender, chat messages are retained as defined in the Data Retention Schedule. The deletion is final and cannot be recovered.
- If a user is deleted, any existing chat messages sent by that user are denoted as unknown user.

Shared Content

- The following content can be for Mitel One specific chats (via Web Chat or social messaging/SMS integration), chat history will be retained for the life of the customer's Mitel One contract. Posted in a direct message, stream, or meeting space:
  - Attachments
  - Voice Message
  - Location
- Shared content is accessible by the participants of direct, stream, and meeting space to which the shared content was attached .
- The creator of the content can delete the content. The delete is final and cannot be recovered.

Data

The data in Mitel One is processed in accordance with Mitel's Privacy Policy. For more information, see Mitel Application Privacy Policy.

Security

This section explains the Mitel One security concerns pertaining to the re-use of a Mitel cloud user account.

You must adhere to the following general guidelines when assigning a Mitel cloud user account, as not observing these guidelines will result in a breach of data and privacy.

- Each Mitel One user in a specific company is assigned a unique user account in a specific Mitel cloud account; ensuring that the user is unique in the overall Mitel Cloud.
- A user can use the same user ID / Mitel cloud user account to access both - the Mitel One web application and the mobile application.
- Each user's Mitel cloud user account has user-specific information that must not be shared

with another user; for example, user name, email, desk phone extension, and mobile number.

- A CloudLink Accounts Administrator onboards users by sending them a welcome email. Users validate their cloud user account by verifying their email address - in some cases their mobile phone number - and providing a password. A user then establishes a secure user account and logs in to the Mitel One application.
- A user's desk phone extension number, name, and email address can be changed; however, the assigned user account cannot be changed. The cloud user account is unique to each user.

Access to Cloud User Account Data

The following data is accessible to users when they log in to Mitel One:

- Voice Call History: Incoming and outgoing call information (when and whom) is specific to each user.
- Message Data: Information in direct messages and streams (including public and private streams) is accessible to all members of the direct message or stream.
- Contacts: Directory information containing name, extension number, and in some cases mobile number and avatar, of every user in the organization.

Sharing of User IDs

Two users sharing a MiVoice Office 400 deskphone is supported with the hot desking feature. However, while sharing, both users can view only their own data; for example, call history.

Two users logging in to the Mitel One application with the same user ID is not supported because this implies two different users accessing and sharing the same single source of data.

You must adhere to the following general guidelines when assigning a Mitel cloud user account, as not observing these guidelines will result in a breach of data and privacy.

- Do not share or re-assign a Mitel cloud user account to different users. Any user, if provided access to another user's account will have access to the call history and direct/private messages sent and received by the latter.
- Changing the user name, email, desk phone extension, and password does not create a new user account.
- Only users of the same organization must be added to a Mitel cloud organization account because the contacts directory for the whole organization is available to every user in an account.

The following scenarios illustrate what could happen, in a hospitality environment, if the above guidelines on sharing a cloud user account are not adhered to:

- If a hotel guest is provided with access to a CloudLink user account previously used by a different hotel guest, the call history and private messages sent/received by the original guest will be available to the new hotel guest.
- If access to Mitel One is provided to hotel guests, every hotel guest will have access to the PBX directory, which includes the names and numbers of the entire hotel staff, making it possible for the guests to contact every member of the hotel staff, rather than just the front desk and guest services.
- The personally identifiable information of hotel guests must be available only to a section of the hotel staff; for example, guest services. However, providing access to Mitel One to the entire hotel staff will allow every member of the hotel staff to see the personally identifiable information (name and email) of every hotel guest.

Managing Meetings

Meetings enables appropriately entitled users to create and join multi-party video conferences and to invite guest users and registered users. Additional safeguards to protect meetings participants are described in the following sections.

Types of Participants

- **Registered User**: a licensed Mitel One user (that is a user who has been provisioned for Meetings services by an account administrator of the entity who subscribes to Meetings). Registered users can create and schedule meetings. They can also verify guest users in the waiting room to allow them to join meetings, remove a user from a meeting, and invite more users into a meeting while it is active. registered users can video meeting, chat, and share files and their screen.
  NOTE: You cannot share your screen if you are using Meetings mobile application.
- **Guest User**: An unlicensed Mitel One user (that is a participant who has not been provisioned for the Meetings service or is not currently logged in to the service.). A guest user joins the meeting through the Web according to directions from the meeting invite they receive and must wait in the waiting room until a registered user allows them entry. Guest users can participate in a video meeting, chat, share files and share their screen.
- **PSTN User**: A user who has only PSTN access can join a meeting as a voice-only participant by using an advertised access dial-in number specified in the meeting invite.
- **Organizer**: The registered user who creates the meeting.
- **Invited Participant**: A registered user that has been invited to attend a meeting by an organizer.
- **Attended Participant**: A registered user or guest that has attended a meeting.

Waiting Room

Guest users must first wait in the Waiting Room, which is a temporary parking spot outside of the meeting. This allows any registered user to verify guest users before allowing them into the meeting by vetting the identity information which the guest provided.
NOTE: The Waiting Room feature is currently not available in Meetings mobile application.

Naming Meetings

It is highly recommended that a meeting be given a unique humanly identifiable name that is easy to remember for the participants. This will enable registered users to easily identify which meeting space to use for their collaboration and facilitate meeting searches.

CAUTION:

- Customers should exercise caution to prevent accidental disclosure of Meeting Access Codes.
- Mitel recommends that at least one participant in a meeting use the Mitel Meetings client to provide visibility to other participants in the meeting.

Meeting Lifecycle

Meetings comprise a virtual collaboration space (the “meeting space”) and 0 or more live audio, video and/or screen sharing collaboration sessions (“live sessions”), which can be recorded. Both the meeting space and the live session have unique URLs.

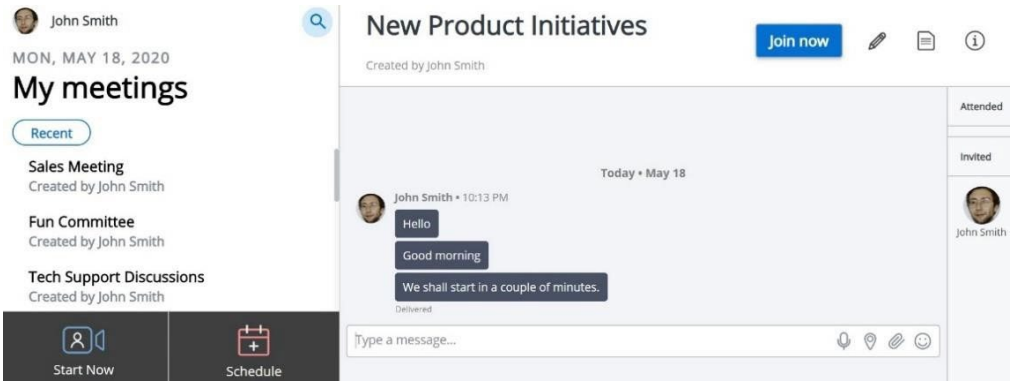

Figure 4: Meeting Space

A meeting space consists of a meeting name, participants, a chat conversation, and files from live sessions. Each meeting space is identified by a unique sequence of nine or more digits (“access code”).

A meeting space is created when the organizer schedules a meeting in the calendar or can be created on an ad hoc basis at any time. In the meeting space, the registered user can schedule and join live sessions, discuss topics via chat, share files, and access recordings of live sessions (chats, shared files, and recordings are individually and collectively “content”).

Invited participants can collaborate in the meetings space prior to the live session, for example the invited participant may attach documents or seed the chat conversation with initial messages.

Meetings are listed on the home page of the organizer as well as on the home page of invited or attended participants. The registered user can hide meetings so that they no longer appear in the list. The organizer can delete meetings, which deletes all the content associated with the meetings deleted. Hiding a meeting does not delete it.

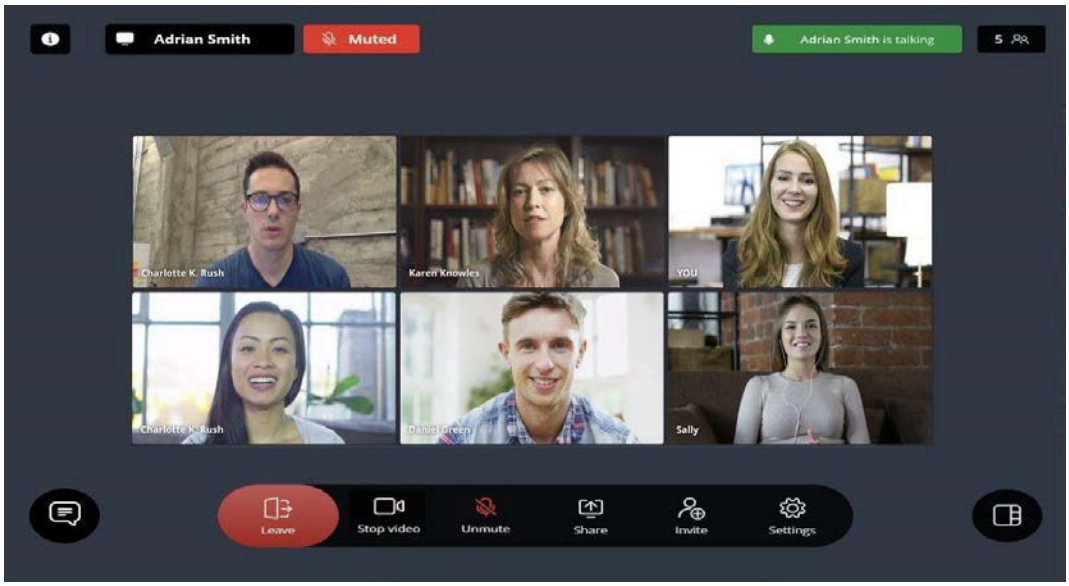

Figure 5: Live Session

All live sessions occur at the same URL. The meeting space URL and live session(s) URLs individually and collectively are referred to as the “meeting URL”. The meeting access code is part of the meeting URL.

Live sessions have a maximum duration of 24 hours.

Content is mirrored between the meeting space and live sessions, where it is available for read/write purposes. Ending a live session does not end or delete the meeting.

CAUTION:

Meetings do not have an expiration date. Meetings spaces, including the live session URL (and the live sessions themselves), are deleted only if the organizer deletes the meeting, or the corporate account which the organizer belongs to is terminated. Content is deleted only as defined in this document.

Access to Meeting Space

Any registered user who obtains a meeting URL or has a meeting access code can enter the meeting space or a live session, at any time. By contrast, a guest, is taken to the waiting room and can enter only a live session upon acceptance by a registered user who is already in the live session, a guest cannot enter a meeting space.

Meeting Recordings

- Recording can be initiated by any registered user in a live session.
- Only the registered user who initiated the recording can stop the recording.
- When a recording is initiated, all participants are notified, including those attending by telephone only. Notifications are presented to new attendees who join a meeting where recording is in progress.
- Recordings are accessible to all registered users via the meeting space and to all registered users and guests during live sessions.
- Any registered user or guest with access to a recording can download the recording for offline viewing and share the downloaded files with others.
- The maximum space available to a registered user in the cloud to store the recordings is 5 GB.
- There is no limit on the duration of recordings, and the system can record to the lifetime of the session.
- Effective July 1. 2021, recordings will remain in the meeting space until the earlier of 12 months from the recording date, or the meeting space is deleted by the organizer. Recording made prior to July 1, 2021, will remain in the meeting space until the earlier of 12 months from July 1, 2021, or the meeting space is deleted by the organizer.

Managing Audio Softphone and Meetings Audio

For privacy, users can choose to mute the microphone by default when joining a Meeting.

CAUTION:

Users should exercise caution using the soft phone while simultaneously participating in a meeting, if the microphone is unmuted inside the meeting, what you say on the phone may be overheard by the meeting participants. For example, disconnect from the meeting before taking or placing a call using the soft phone.

Security and Privacy of a Meeting

For security and privacy purposes, it is recommended:

- not to re-use a Mitel cloud user account for different users.

- not to re-use meetings unless the meeting is a re-occurring meeting with the same group of participants. The reason is that content is accessible to all participants and if the meeting is re- used for a different purpose and/or with a different group of participants, there may be details in the content that should not be shared across groups. Also new participants will have access to previous recordings, for example, chat log or shared files.
- consider deleting the meeting after the live session has finished and any attachments/recordings have been downloaded by any participants that need those artifacts.
- consider deleting files, recordings, and chat messages appropriately to address invitee and attendee changes.
- assess whether it is appropriate for participants to be able to edit/delete messages and set admin setting accordingly.

Audit Logs

For security and regulatory purposes, Mitel may capture the following types of meeting metadata: Initiator's and each participants' name and user name (as applicable), phone number and IP address and IP port number as applicable, location, conference date, time and duration, chat, chat edit, chat delete date and time, location, network path, details of any files exchanged including file size, file edits and deletes, call recording size, start, stop, and deletion and location of system used.

Storage Location[1]

Account Cloud Region	Storage Location
Europe/EEA	Europe/EEA
United States	United States
Canada	United States
Australia	Australia

[1]Location set out herein are default locations but are not absolute.

Hosts and Ports Required to Support Mitel One

For information about the performance profile and network requirement prerequisites, see the following sections in the CloudLink Gateway User Guide.

- Configuration Prerequisites
- Network View
- Mitel One web
- Mitel One mobile

Product Hardening for Ensuring Security during Product Development

During the Mitel One Application Development Cycle, all unnecessary diagnostic and debug software is removed from the released version of the software.

The software delivery process and change management policy are extensively automated through multiple Continuous Integration / Continuous Deployment (CI/CD) pipelines to allow deployment into development and production environments. The automated process includes code reviews and execution of automated testing and supports the separation of duties. Security best practices are implemented through configuration options.

Mitel One application undergoes Software Composition Analysis and Vulnerability scans regularly.

Security and privacy threats are constantly evolving. To combat these threats, product designers need to continuously evaluate product security risks and ensure that robust controls are included in the design. The practice of evaluating security risks and incorporating protective measures in the design must be an integral part of the product design process itself.

Mitel's Secure Development Life Cycle (MiSDLC) policy was created to ensure that product developers will employ the latest information security and privacy best practices throughout the product development process.

Mitel One application Release 1.0 was developed in accordance with Mitel's Secure Development Life Cycle policy, which was created to ensure that web applications are designed with best practice safeguards to mitigate risks to confidentiality, integrity, availability of data contained within the web application, and to all data related to the functionality provided by the web application in mind.

Mitel’s Secure Development Life Cycle (MiSDLC) is described in the paper found at the following URL.

https://www.mitel.com/en-ca/document-center/security/technical-papers/all-releases/en/mitel-secure- development-life-cycle-version-10 .

The paper provides an overview of the customer benefits and the key aspects of MiSDLC. This paper also covers the key components of Mitel’s Product Security Incident Response Process (PSIRT).

Patches and Updates

The latest security updates and patches are automatically made available to the clients. For the web portion of the client, the web client is automatically updated to the latest recommended. For scenarios where end user permission is required for an update, the user will be prompted for permission to update to the recommended software version.

Mitel Product Security Policy

The Mitel Product Security Policy describes how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how reporting of security vulnerabilities is provided. The Policy is available here: www.mitel.com/support/security-advisories/mitel-product-security-policy .

Mitel Product Security Advisories are available here: www.mitel.com/support/security-advisories .

Appendix A – Definitions and Glossary

AES: Advanced Encryption Standard. A specification for electronic data encryption adopted by the U.S. government to protect classified information. The algorithm used by AES is a symmetric-key algorithm; that is, the same key is used for both encrypting and decrypting the data.

Audit trials: A series of documents, computer files, and other records that are periodically examined to track how transactions are handled and to identify conditions that call for actions to be taken.

Authentication: The process by which a system ascertains that a person or entity trying to access it is actually the person or entity it claims to be.

Cloud app user: An app user licensed in CloudLink and belonging to a specific registered account.

HTTPS: Hypertext Transfer Protocol Secure. It is the secure version of the standard Hypertext Transfer Protocol, the protocol that web browsers use for communicating with websites.

Network threats: Attempts by attackers to execute commands designed to intercept traffic traversing a network or to disrupt normal operation of a network. These attacks typically involve breaching a company's infrastructure by exploiting software vulnerabilities to execute such commands.

Open ID Connect: An authentication protocol that enables clients to verify the identity of the end-user based on the authentication.

Product hardening: The process of reducing vulnerability in applications, systems, infrastructure, firmware, and other areas by pre-empting potential attack vectors and limiting the system's vulnerability surface.

Reducing vulnerability typically includes changing default passwords; removing unnecessary software, user names, or logins; and disabling or removing of unnecessary services.

PSTN: Public Switched Telephone Network. It comprises the world's telecommunications infrastructure including systems, devices, transmission lines, and networks, interconnected through switching centers to enable telephones to communicate with one another.

MiSDLC: **Mitel Secure Development Life Cycle**. An application development approach in which security is treated as a continuous concern in all phases of application development. In SDLC, security-related procedures such as penetration testing, code review, and architectural analysis are an integral part of the development schedule.

TLS: Transport Layer Security. A security protocol that provides privacy and data security for communications over the Internet. TLS encrypts all communication between web applications and servers. TLS can also be used to encrypt other communications such as email, chat, and voice.

CloudLink Gateway: Mitel CloudLink Gateway solution that allows Mitel CloudLink Platform to communicate with Mitel PBX (communication system).

DISCLAIMER

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of Mitel One and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.